UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,360	12/03/2003	Paul Funk	1014-228US01	6376

7590 06/28/2007

Kent J. Sieffert
Shumaker & Sieffert, P.A.
1625 Radio Drive
Suite 300
St. Paul, MN 55125

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
06/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/728,360	FUNK, PAUL	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-87* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-87* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 December 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/20/04, 6/29/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-87 have been examined.

Priority

2. The instant application claims priority to Provisional U.S. Patent Application No. 60/430,398, filed 3 December 2002.

Information Disclosure Statement

3. The following Information Disclosure Statements in the instant application have been fully considered:

IDS filed 20 January 2004.

IDS filed 29 June 2004.

Drawings

4. The drawings are objected to because in several figures there exist large gaps in the labels that obscure the meanings of the labels (see figure 2, item 206, for example).

5. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

6. The use of the trademark Java and several trademarks on p. 36, lines 18-19 and p. 38, lines 11-14 have been noted in this application. They should be capitalized wherever they appear and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Objections

7. Claims 3, 21, 72, and 80 are objected to because of the following informalities:

In the first paragraph of each claim, it is unclear whether "standard Message Digest 5 algorithm" refers to the MD5-based function of claim 2, or this paragraph rather recites that manner in which the MD5-based function differs from standard MD5. It is being presumed that MD5 as modified in this paragraph is the MD5-based algorithm.

Appropriate correction is required.

8. Claim 77 is objected to because of the following informalities: The claim ends with two "period" marks. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claim 86 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The claim is a single means claim, which is non-enabling. See MPEP 2164.08(a).

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 12, 13, 30, 31, 49, 50, 62, and 63 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 12, 30, 49, and 62 recite the limitation "the plurality of sequences" in p. 42, line 5 et al. There is insufficient antecedent basis for this limitation in the claim. It is being presumed that this refers to the issued challenge.

Claims 13, 31, 50, and 63 depend from rejected claim 12, 30, 49, and 62 and include all the limitations of those claims, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1, 2, 4-10, 12, 16, 18-20, 22-28, 30, 34, 36-47, 49, 52, 54-60, 62, 65, 67-71, 73-79, 81-83, and 85-87 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,751,812 to Anderson.

As per claims 1, 4-6, 16, 19, 22-24, 34, 38, 40-47, 52, 54-56, 65, 68, 70, 73, 74, 78, 81, 82, and 86, Anderson discloses a system in which a server challenges a client to authenticate a user, and receives a partial hash ($H^{i-1}(A)$) as calculated by the client in response. The server then completes the hash computation by computing $H(H^{i-1}(A))$ to calculate and verify $H^{i}(A)$, where A is a user password (see column 5, lines 51-56). The client and server together perform i iterations, with the client performing i-1 iterations and the server performing 1 iteration.

Regarding claims 39, 69, and 87, in order to be loaded on the computers, the process must be encoded onto a computer-readable medium.

As per claims 2, 20, 71, and 79,Anderson discloses the use of MD5 for the hashing algorithm (see column 5, line 46).

As per claims 7-10, 25-28, 45-47, 57-60, 75, 76, and 83,the number of iterations is part of the password credential, and the number of bits is therefore transmitted during the initialization or password changing process (see column 5, line 65 to column 6, line 19). The number of iterations so determined mandates the state and length of any

partial hashes. Since the number of iterations is selectable, this governs the entropy of the challenge.

Regarding claims 12, 30, 49, and 62, valid passwords inherently contain at least one non-zero bit.

Regarding claims 18, 36, 37, 67, 77, and 85,the communication channels being used constitute tunnels.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 11, 13, 14, 17, 29, 31, 32, 35, 48, 50, 51, 53, 61, 63, 64, and 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,751,812 to Anderson.

Regarding claims 11, 29, 48, and 61, Anderson does not disclose the use of padding.

Official notice is given that it is well-known in the art to add padding, the number of bits being dependent on the size of the field, to a field to fit it in a standard format.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to add padding according to the number of bits necessary to fill out the block, and it would also be obvious that, in some implementations, there would be 63 bits of padding.

Regarding claims 13, 31, 50, and 63, Anderson does not specifically state that data is organized in octets.

Official notice is given that it is well-known in the art to organize data in octets (a.k.a. bytes), in order to efficiently conform to the operating efficiencies of computers.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to organize the sequences in octets, as is well-known in the art in order to efficiently conform to the operating efficiencies of computers.

Regarding claims 14, 32, 51, and 64, Anderson does not disclose the necessary password lengths.

Official notice is given that it is well-known in the art to set minimum lengths for passwords, as short passwords are easy to crack.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Anderson by setting a minimum number of octets in the password sequences, as is well-known in the art, as short passwords are easy to crack.

Regarding claims 17, 35, 53, and 66, Anderson does not disclose the transmission of the hash to a third network device.

Official notice is given that it is well-known in the art to transmit authentication information to a system administrator for verification, in order to allow the system administrator to have control over the network.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Anderson by sending the hash value to a network administrator in order to allow the system administrator to have control over the network.

13. Claims 3, 15, 21, 33, 72, 80, and 84 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,751,812 to Anderson as applied to claims 1, 2, 19, 20, 71, 78, and 79, above, and further in view of U.S. Patent No. 6,901,512 to Kurn et al.

Anderson does not disclose the adding of additional information in addition to the password as part of the challenge.

Kurn discloses the adding of algorithm information and a salt to an authentication argument (see column 19, lines 52-54), as these fields are necessary for proper recovery of a shared secret.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Anderson by adding a salt and algorithm information to the authentication argument, as disclosed by Kurn, as these fields are necessary for proper recovery of a shared secret.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand, can be reached at (571) 272-3811.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Matthew Heneghan/

June 21, 2007 Patent Examiner (FSA), USPTO Art Unit 2134